



# Human Systems IAC GATEWAY

Published by the Human Systems Information Analysis Center



## Human Factors in Homeland Security

Sandra G. Hart

As the nation focuses its attention on meeting the daunting challenges that fall under the umbrella of "homeland security," government agencies, industry, and academia have been implementing solutions to some of the most immediate problems and defining longer-term research to address more challenging, long-range issues. The following articles were selected to provide different perspectives on the role that the field of human factors should, has been, and will play in meeting these national objectives.

The role that human factors might play is summarized in excerpts from a national research agenda developed by the National Academies Committee on Science and Technology for Countering Terrorism. Drury, Hancock, Hart, and Endsley suggest ways in which human factors research originally conducted with other appli-

cations in mind, could be applied to support the human operators in emerging systems so the system will work as well as intended. And, Mumford suggests just a few of the avenues through which such scientific knowledge can be made available to the people who need it. Immediate and near-term actions already initiated by airlines, pilot associations, and manufactures are described in the articles by Canto and Wright. Different roles the federal government is playing is described by Chelette (application of basic research and commercialized technologies developed or funded by government agencies to the war on terrorism), Bellenkes (the role of committees in

*continued on next page...*

## inside:

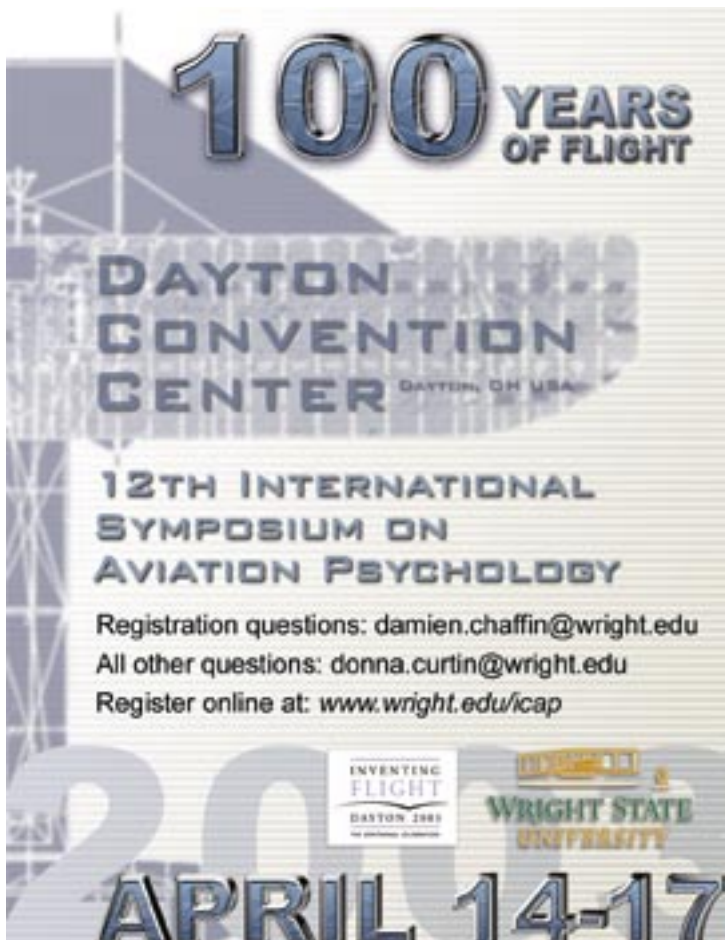
- 3 The Role of Science and Technology in Countering Terrorism
- 4 A Unified Model of Security Inspection
- 5 Vigilance and the Price of Freedom
- 6 A Safe and Secure System
- 7 Bringing to Light the Meaning of Information
- 8 Advocating for Human Factors
- 9 Airbus Aircraft Security
- 10 Security Initiatives of the ALPA
- 11 Air Force Applications to Aviation Security Issues
- 12 Special Working Group on Human Factors in Homeland Defense
- 13 Human Systems Technology and Aviation Security
- 14 Calendar
- 16 The Human Factors of Civil Aviation and Transportation Security
- 17 Lessons Learned
- 18 Police Performance and Human Factors Research
- 19 Improvement of Building Evacuations
- 27 Products



The Human Systems IAC is a United States Department of Defense Information Analysis Center administered by the Defense Technical Information Center, Fort Belvoir, VA, technically managed by the Air Force Research Laboratory Human Effectiveness Directorate, Wright-Patterson Air Force Base, OH, and operated by Booz Allen Hamilton, McLean, VA.

The appearance of an advertisement in this newsletter does not constitute an endorsement by the Department of Defense or the HSIAC.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 01-01-2003		2. REPORT TYPE Newsletter		3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2003	
4. TITLE AND SUBTITLE Gateway XIII 4 Unclassified				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Hart, Sandra G ; Drury, Colin G ; Hancock, Peter A ; Szalma, James L ; Endsley, Mica et.al. ;				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME AND ADDRESS Human Systems IAC 2245 Monahan Way Bldg 29 WPAFB, OH45433-7008				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS ,				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE ,					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT This newsletter contains articles on the following: The Role of Science and Technology in Countering Terrorism; A Unified Model of Security Inspection; Vigilance and the Price of Freedom; A Safe and Secure System; Bringing to Light the Meaning of Information; Advocating for Human Factors; Airbus Aircraft Security; Security Initiatives of the ALPA; Air Force Applications to Aviation Security Issues; Special Working Group on Human Factors in Homeland Defense; Human Systems Technology and Aviation Security; The Human Factors of Civil Aviation and transportation Security; Police Performance and Human Factors Research; and Improvement of Building Evacuations. The newsletter also contains a calendar of human factors events as well as HSIAC products.					
15. SUBJECT TERMS HSIAC collection; Human Factors; Aircraft Security; Civil Aviation; Transportation Security; Police Performance; Research; Building Evacuations					
16. SECURITY CLASSIFICATION OF:  a. REPORT    b. ABSTRACT    c. THIS PAGE Unclassified    Unclassified    Unclassified		17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 28	19. NAME OF RESPONSIBLE PERSON Darrah, Sara Sara.Darrah@wpafb.af.mil	
				19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number DSN	
				Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18	



...continued from previous page

sharing ideas, coordinate implementation of solutions), Steele (the role of DoD), and Neiderman (recent and planned human factors activities being undertaken within the Transportation Security Administration to improve airport security). Articles by Zedlewski and Vila focused on the role of law enforcement, especially lessons we can learn from first responders to September 11<sup>th</sup>, the role of the federal government in supporting state and local governments, and challenges created by shortages of qualified police officers and equipment in need of better human factors. Groner deals with post-disaster responses, focusing on improving building egress.

These fourteen articles offer just a sampling of the many different roles that human factors professional might play in preventing future terrorist attacks, coping with such events should they occur again, and mitigating the consequences. By working with government agencies and industries most directly involved in promoting national security, the field of human factors can demonstrate its relevance and value yet again. ■

## Visit the newly redesigned HSIAC web site!



<http://iac.dtic.mil/hsiac>

The recent redesign is intended to transform our site into a knowledge portal for information related to Human Systems Integration (HSI) and Human Factors Engineering (HFE). The initial design is supported by active web pages, but the long-term goal is to have a robust database.

HSIAC is also seeking high-quality web resources related to HSI and HFE. We invite you to suggest resources to add. Please submit them to [julie.chitwood@wpafb.af.mil](mailto:julie.chitwood@wpafb.af.mil) along with your name and phone number.



# Human Factors Issues in the National Academies Report Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

National Academies of Science

In June of 2002, the National Academies released *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. This report identifies actions, including deployment of available technologies, that can be taken immediately, and it points to the urgent need to initiate research and development activities in critical areas. Understanding human factors will be an essential step in successfully implementing any new counterterrorism technology, and the importance of taking human factors into account in the design of all systems, particularly those used by first responders, is a general principle underlying many of the recommendations made in the report.

Virtually all technologies are subject to the reality that human agents and social organizations are necessary to implement and operate them. Thus a key aspect in the effective deployment of any of the technologies discussed in this report is the ease and effectiveness of use of information and other technical outputs by the people they are intended to support. Often, the weakest part of the system is the (frequently neglected) human link. Overlooking the human element can make it more difficult for people to do their jobs and, ironically, significantly reduce the effectiveness of the security technologies. In the worst case, the entire system may be rendered useless. Thus, human-centric design and an improved understanding of the factors that contribute to systematic human errors are essential.

Research is needed so that appropriate, informed decisions about deployment of new counterterrorism technologies can be made. Whether a security system will be effective depends on how the system is used, by whom, and for what ends. If the primary purpose is deterrence, the needed technical capabilities of the system are different than if it is for warning of potential attacks or for controlling access to an area. The background and training of users could also vary widely (e.g., border security guards, first responders, or

decontamination specialists), so user interfaces must also be based on the best human factors research. This will be a particular issue in the design and implementation of sensor systems for the detection of various threats, such as biological or chemical agents, nuclear materials, explosives, or conventional weapons.

One example of an area where human factors will be particularly critical is in the development and deployment of security system concepts for use in transportation systems, such as the design of airport security checkpoints that are more efficient and less error-prone. Human factors expertise is necessary for crafting layered security systems that, as a whole, increase the perceived risk of getting caught and maximize the ability of security personnel to recognize unusual and suspicious patterns of activity and behavior. Recognition of human factors is important for ensuring that the role of people in providing security is not determined by default on the basis of what technology promises, but rather as a result of systematic evaluations of human strengths and weaknesses that technology can both complement and supplement. Indeed, it may turn out that some technologies do not hold promise because they are inferior to, or incompatible with, the performance of human users—for instance, they might interfere with the performance of flight crews, bus drivers, or screeners. Thus expertise and research on human factors will need to be one of the key elements of the new Transportation Security Agency's programs. ■

This article may be ordered from the National Academies Press at (888) 624-7645 or (202) 334-3313 or online at <http://www.nap.edu/catalog/10415.html>. The report is also available on the web at: <http://books.nap.edu/html/stct/index.html>

*Making the Nation Safer* was written by a National Academies committee co-chaired by Lewis M. Branscomb, Emeritus Professor of Public Policy and Corporate Management and Emeritus Director of the Science, Technology, and Public Policy Program, Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, and Richard D. Klausner, Executive Director of Global Health, Bill and Melinda Gates Foundation. The report is a product of the work of one hundred and eighteen people on a parent committee and eight panels; the authors' expertise covered a wide range of relevant areas, including systems engineering, bioterrorism, and transportation systems security.

<http://iac.dtic.mil/hsiac>

# A Unified Model of Security Inspection

Colin G. Drury, Ph.D.

*Colin G. Drury, Ph.D., is UB Distinguished Professor of Industrial Engineering, University at Buffalo, SUNY. He is a member of the National Research Council and Federal Aviation Administration Committees responsible for transportation security.*

A major part of homeland security policy still focuses on detection of threats before they can harm the public. Particularly for various modes of public transportation, an array of equipment and procedures has been developed for threat detection. These are challenged by an ever-expanding set of threat objects that range from weapons to improvised explosive devices and chemical and biological agents. Each threat-detection system is composed of humans and machines. Typically, each system is designed as a stand-alone measure with specific performance objectives (e.g., probability of detection, probability of false alarm and resource use/throughput time) and very specific applications of human factors (e.g., the design of an operator interface or development of a training program). Unfortunately, system designers often use only a fraction of the available human factors knowledge base, largely because they do not know that such a knowledge base exists beyond meeting written customer requirements.

A model of how human operators and automated components cooperate to provide security inspection is proposed. The model is based on a generic description of inspection operation functions in security as well as many other domains such as manufacturing and aviation maintenance. The functions of inspection are set-up, present, search, decide, and respond. Each function provides a link between the actual task and existing quantitative knowledge about human and automation performance (e.g., visual search theory or various decision theories). The model applies to x-ray screening, bulk explosive detection, trace element detection, hand searches and even remote surveillance.

With a unified model, we can begin to link overall errors (e.g., misses, false alarms, delays) to potential reasons for these errors (e.g., skill-based search failures or rule-based mistakes). We can also demonstrate that decisions about how to allocate the generic functions between human and machine can be based on performance predictions. This allows customers, designers, and developers to focus innovation on system needs, as a complement to more traditional, technology-driven approaches to automation. It also allows system designers to consider a wider variety of human factors design interventions, thereby improving threat inspection and, ultimately, homeland security. ■

## E-mail?

Would you like to receive your copy of *GATEWAY* by E-mail?

If so, please E-mail your address to [roseann.venis@wpafb.af.mil](mailto:roseann.venis@wpafb.af.mil).

For more information please contact:

Colin G. Drury, Ph.D.  
University at Buffalo, SUNY  
Department of Industrial Engineering  
342 Bell Hell Hall  
Buffalo, NY 14260

# Vigilance and the Price of Freedom

Peter. A. Hancock  
James. L. Szalma, Ph. D.

When we have to act as a concerted group or use a common convenience, such as mass transportation then individual freedoms come into conflict with collective rights. Conjoint and reciprocal security intrinsic to social interaction is being sought now more visibly in aviation and somewhat less visibly in other forms of transportation and communication. Perhaps in advancing security in their own realm, aviation professionals can set the common example. The fundamental challenges for human factors in security are to:

1. Devise ways of distinguishing what potential and actual sources of communal threat exist
2. Provide valid and accurate assessment methods to distinguish such threats
3. Indicate avenues of action by which threats can be excised or rendered harmless.

To meet these challenges, we suggest three avenues to pursue in our collective efforts to combat terrorism:

1. Improve personnel selection and training
2. Design of systems to support sustained attention or vigilance
3. Possible control of aircraft beyond the cockpit alone.

In the present NAS, the pilot is in control and responsible, although control is also mediated by air traffic personnel who provide guidance and direction. Thus, one role of vigilance lies in the selection and the training of flight deck and ATC personnel to deny individuals who seek to usurp control for nefarious purposes access to air traffic control facilities and the commercial flight deck. Since this function has not yet failed, to our knowledge, political will is likely to be slow to react to this potential threat over known threats. Inevitably, concern has focused on public access to the flight-deck as this was the approach used by the September terrorists. In addition to

physical barriers erected to exclude unauthorized individuals from entering secure areas, selection barriers must be erected for other individuals who work in the system and for whom the everyday vigilance of passenger control is easily circumvented. Security background checks and cross-referencing with emergent National databases should provide help in this regard with support from human factors professionals who are experienced in dealing with the problem of information overload. Screening personnel with ground access to aircraft and control facilities as well as those who fly in a professional capacity or have privileged access (e.g., flight attendants, Federal Air Marshals) will be a Herculean task.

The field of human factors considers the security problem as one of distinguishing signal from noise. In this context, the signal is the source of threat (a person or what he possesses) and the “noise” (or, more properly, the non-signal) all other forms of non-threats. Since the occurrence of threats are so rare, and non-threats so predominant, the detection process fits the scientific definition of vigilance (see Warm, 1984). A quintessential component of laboratory vigilance tasks is “event rate”, or how often stimuli are presented to observers. In the case of passenger screening, this might be the number of people who pass through a detector per unit time. Embedded in event rate is “signal rate” or the proportion of events that are targets. In laboratory testing, realistic event rates are presented (e.g., one event every

*continued on page 20...*

*Peter Hancock is Provost Distinguished Research professor in the Department of Psychology, the Institute for Simulation and Training, and at the Department of Civil and Environmental Engineering at the University of Central Florida. He currently holds a courtesy appointment as a research scientist at the Massachusetts Institute of Technology (MIT) and as an Adjunct Senior Research Scientist at the Transportation Institute of the University of Michigan. Professor Hancock is the author of over four hundred referenced scientific articles and publications as well as editing numerous books. His theoretical works concern human relations with technology and the possible futures of this symbiosis.*

*Jim Szalma holds a Ph.D. from the University of Cincinnati in experimental psychology and has been a faculty member at Farmington on Long Island. He has just joined the University of Central Florida MURI-OPUS group where he directs a number of projects concerning stress and performance response. His particular expertise is on vigilance and response capacity, and he has published a number of papers in this area.*

<http://iac.dtic.mil/hsiac>

# A Safe and Secure System



Sandra G. Hart

*Sandra Hart is the Special Advisor for Strategic Planning to the Chief of the Human Factors Research and Technology Division at the National Aeronautics and Space Administration (NASA) Ames Research Center. She has worked in the field of aviation human factors for more than thirty years.*

**T**he field of human factors has much to contribute to the national goal of preventing future terrorist attacks against the flying public:

1. Tools to predict the impact of proposed changes in equipment, procedures, and regulations on system efficiency and effectiveness
2. Human-centered techniques for designing interfaces and analyzing task and system requirements to allocate functions optimally among humans and technologies
3. Improved training and selection approaches.

Human factors can serve as a line of defense against hastily designed or implemented security measures that inadvertently threaten aviation safety. In fact, lessons learned from the successful application of human factors to aviation safety might offer valuable insights about challenges that must be overcome to ensure aviation security.

For half a century, the aviation community has identified potential failure points and threats based on research, operational experience, and analysis of accident and incident data. Engineers identified and reduced the likelihood of single-point failures of aircraft structures, avionics, controls, linkages, and displays and elements of the ground-based infrastructure. Human factors researchers identified and tried to eliminate the causes and consequences of human errors in the air and on the ground. Many disciplines worked to

reduce threats from the physical and operational environment in which aircraft operate.

Recent safety improvements have benefited from the growing recognition that patterns or sequences of events in combination threaten aviation safety more than do individual failures of human, machine, or system. In commercial aviation, layers of protection such as triply redundant flight critical hardware and software, hardware and software reliability requirements, layers of automation backed up by manual reversion modes, standard operating procedures, checklists and crosschecks, stringent training and qualification standards and conservative certification processes have resulted in fewer accidents. However, the percentage of these accidents attributed to “human error” has remained stubbornly high. These layers of protection are redundant, parallel, and independent; one pilot cross-checks the other, pilots monitor automated subsystems, air and ground systems detect deviations from the plan or values that exceed vehicle, human, or system safety margins. By design, they offer many opportunities to prevent, detect, remedy or mitigate failures, making it most unlikely that multiple risk factors will occur in close succession and combine unopposed to create a nonrecoverable failure. Thus, the rare accidents that do occur often represent the nearly random co-occurrence of events, some of which might have had little impact under other circumstances. Although historical rates of accident types and causes can be computed and actual statistics projected it is impossible to predict precisely when another accident will occur.

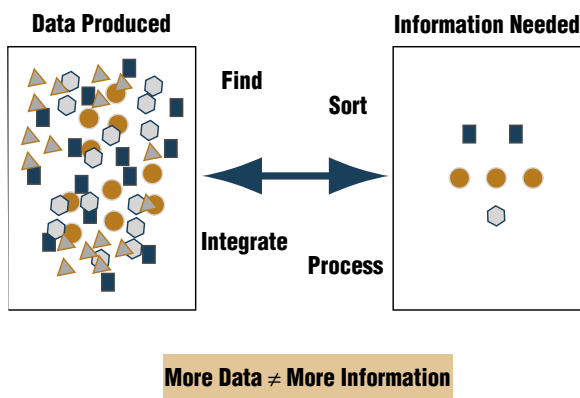
The situation is somewhat different in aviation security, although it is equally important to the reliability and economic viability of commercial aviation. Security has received less attention than safety, primarily because there have been few successful challenges to the national airspace. Well-documented failures of checkpoint screeners, the low rate of checked-baggage scanning, and the

*continued on page 21...*

# Breaking through the Data Glut: Bringing to Light the Meaning of Information

Mica Endsley

**T**oday, it is possible to gather and transmit vast quantities of data. However, this unprecedented access to data has failed to produce hoped for leaps in understanding because there is a huge gap between the glut of data produced and disseminated and users' abilities find and process the information they really want amongst all that is possible (see Figure 1). This gap challenges many in positions crucial to security and homeland defense—the intelligence analyst who may read thousands of messages to unearth a terrorist plots, an American soldier who must integrate and coordinate the activities of widely distributed units in a foreign country surrounded by hostile combatants as well as civilians, and millions who need to be able to detect information attacks by hackers. Just as information is a tool in our arsenal, it also serves as a tool of those who seek to undermine the U.S. and its institutions.

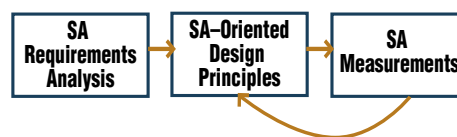


**Figure 1. The Information Gap (from Endsley, 2000b)**

A central truth of the post-technological age is that success (and even survival) depends on rapidly sorting through, understanding and assimilating vast quantities of data; "...only those who have the right information, the strategic knowledge, and the handy facts can make it" (Bennis, 1977). To create systems that support people in this highly

critical task, it is necessary to understand how people process and utilize information in their decision making activities. Incoming data from technological systems, the environment, fellow team members, and others must be brought together as an integrated whole understood by the individual. Situation awareness (SA) is a term used to represent this internalized mental model of the current state of the environment. This integrated picture is the central organizing feature around which all decision making and action takes place. Thus, although the key to coping in the information age is developing systems that support SA, the failure of current technologies to do so leaves human operators, analysts and system users vulnerable to error.

A key benefit of focusing on SA is that it tells us how to combine and understand data. Instead of loading decision makers with hundreds of pieces of miscellaneous data provided haphazardly, SA requirements tell system designers how to bring that data together to form meaningful integrations and groupings that can be easily absorbed and assimilated in time-critical situations. The SA-Oriented Design process (see Figure 2) provides a means to improve human decision making and performance by optimizing SA in system design (Endsley, Bolte, & Jones, in press). This method has been



**Figure 2. The SA-Oriented Design Process**  
*continued on page 22...*

*Mica Endsley is president of SA Technologies in Marietta, Georgia, where she conducts research in the areas of situation awareness, decision making, and integrating humans with automation. She is involved in developing advanced user interfaces for command and control, medical and aviation operations.*



# Advocating for Human Factors

Geoff Mumford, Ph.D.

*Geoff Mumford, Ph.D., is Director of Science Policy for the American Psychological Association (APA). He is a behavioral pharmacologist by training and a private pilot with vested interests in aviation safety and security.*

Much of what we did after September 11, 2001, was simply an extension of what the American Psychological Association (APA) Science Policy Office does day to day—get scientific information into the hands of people who can make use of it. But now the goal was to make sure that Congress and emerging agencies and departments were aware of what existing human factors research might suggest about how to proceed. This included thinking about how to incorporate human factors research into the next generation of security measures and how to improve the infrastructure for conducting human factors research for the future.

By the end of September 2001, dozens of congressional committees and subcommittees were vying for jurisdiction over a large number of counter-terrorism initiatives. Revising transportation security in general and airline security in particular was at the top of the congressional counter-terrorism agenda. Many human factors researchers responded to calls for vignettes about how their findings might help solve existing security problems or shape a security research agenda. We further condensed that information into briefing materials for interested congressional staff. House and Senate versions of an aviation security bill (H.R. 3150 and S. 1447, respectively) sought to optimize the effectiveness of security screening operations, but differed over how to manage the security-screening workforce. The President signed the compromise legislation that called for federalizing the workforce into law (P.L. 107-71) on November 19, 2001.

We are indebted to the many psychologists who accompanied us on multiple visits to meet with congressional staff on Capitol Hill to explain their research as the legislation was evolving.

Involving scientists in those informal meetings was one mechanism by which we tried to infuse human factors research throughout the process, but a formal mechanism was also in the making. The Aviation and Transportation Security Act called for the establishment of a Scientific Advisory Panel to “...review, comment on, advise the progress of, and recommend modifications in...” Transportation Security Administration (TSA)-funded research and development. In February 2002, APA nominated a dozen psychologists with expertise in human factors research to be considered for that panel. In March 2002, we received a reply from the Undersecretary’s office indicating that the Security Subcommittee of FAA’s Research and Engineering and Development Advisory Committee (REDAC) would form the foundation of the new Panel. We are pleased to note that Dr. Colin Drury, a contributor to this edition of *Gateway* is on that panel. As of press time, however, it was unclear when additional members would be named and how TSA would deal with multi-modal oversight issues.

The TSA legislation authorized a fifty million dollar annual research appropriation. Although much was allocated for the deployment of new technologies, the bill also called for the Federal Aviation Administration to consider establishing higher education and training centers for all aspects of aviation security and safety. Presumably, there would be a strong emphasis on applied human factors research in those settings. How TSA might evolve further as part of the new Department of Homeland Security remains to be seen. We are working to reinforce the importance of human factors research with the core of that proposed department by regularly visiting staff leftover from the Office of Homeland Security. They appear to be

*continued on page 22...*

# Airbus Aircraft Security

Captain Rudy Canto

**W**ith safety as its prime concern, Airbus set up an aircraft security task force immediately after the tragic events of September 11. Since then, the task force has been working diligently with customers and actively contributing to industry and government task forces in the United States, and Europe to minimize risks related to the threat of terrorism in air transports by identifying and investigating solutions that could be implemented in the very short term, as well as medium and longer term. In parallel to the task force activity, Airbus initiated a series of meetings with representatives from airline associations, sixty airlines, five airworthiness authorities, and other manufacturers in the U.S. and Europe to review aircraft security improvements.

Airlines and the authorities reacted positively to various Airbus proposals to enhance aircraft security. For example, the Airbus proposal for reinforcing cockpit doors on single-aisle Airbus aircraft was reviewed and approved by the Federal Aviation Administration (FAA), DGAC, European Joint Aviation Authorities (JAA) and other regulatory authorities. Airbus has since issued detailed design plans and associated service bulletins and kits for the cockpit door modifications. Similar modifications were developed for other Airbus aircraft and conversion kits were made available to all customers for in-service aircraft by May 2002. Downtime to retrofit in-service aircraft was kept to an absolute minimum; airlines could retrofit a door on Airbus single-aisle aircraft within forty-eight hours. Aircraft from the production line have been fitted with the doors as standard since August 2002. All associated certification and engineering costs were assumed by Airbus. The new cockpit door protects the flight crew from unauthorized entry while also delivering a number of safety contingencies. It features reinforced attachments, a reinforced and bulletproof main door panel, an escape panel, electrical door latching, an electronic entry pad located in the cabin, and a warning light and buzzer in

the cockpit. In addition, a toggle control in the cockpit enables the crew to control access to the cockpit and secure the door in case of need.

The new cockpit doors are just one of a series of complementary measures being made available by Airbus. These also include a stand-alone video camera system that allows the flight crew to monitor the cabin area outside the door from the cockpit. The full provisions for this system are being installed as standard on all Airbus aircraft. In addition, Airbus developed two approaches for ensuring that the transponder signal from an aircraft to air traffic control cannot be interrupted in the event of an attack. And, to further improve communication between cabin and cockpit crews, Airbus has found a way for each to alert the others should an emergency situation arise. ■

*Captain Rudy Canto is the Director of Flight Operations Technology for Airbus North America. He has worked as a production test pilot, instructor pilot, check airman, and senior management pilot on numerous large transport category aircraft for more than thirty years, and holds a bachelors degree in mechanical engineering from the University of Florida.*

## addresses needed!

If your address label does NOT include a complete street address, P.O. Box, or ZIP code, please provide us with this information. We are trying to comply with the regulations of the U.S. Postal Service. Without this information we cannot guarantee your continued receipt of the Human Systems IAC GATEWAY. Please E-mail changes to [roseann.venis@wpafb.af.mil](mailto:roseann.venis@wpafb.af.mil) or mail changes to:

Human Systems IAC GATEWAY  
AFRL/HEC/HSIAC, Bldg. 196  
2261 Monahan Way  
WPAFB, OH 45433-7022

<http://iac.dtic.mil/hsiac>

# Human Factors-Related Security Initiatives of the Air Line Pilots Association



Jerry Wright

*Jerry Wright is the Manager of Security and Human Performance for ALPA where he has been employed for fifteen years. He holds a Bachelor's Degree from Auburn University and the designation of Certified Protection Professional from the American Society of Industrial Security. He is a flight instructor.*

**T**he events of September 11 awoke the U.S., indeed the world, to the reality of a new type of terrorism. Even today, it continues to threaten the global economy and, more specifically, the airline industry. The violent hijackings of four jetliners resulted in billions of dollars in property damage and other impacts on the North American economy, and led to the slaughter of more than 3,000 innocent people. One of the enduring lessons from those attacks is that the aircraft flight deck must be protected at all costs to prevent future devastation.

After September 11, the Air Line Pilots Association, International (ALPA) led the industry with security recommendations aimed at protecting the traveling public, aircrews, and the airline industry from future terrorist attacks. ALPA played a leading role on the Secretary of Transportation's Rapid Response Teams for Aircraft and Airport Security and made numerous recommendations ultimately adopted by the Department of Transportation. ALPA was asked to testify several times on Capitol Hill in the weeks immediately following the September attacks and presented a "blueprint" for a new security system, many components of which were incorporated into the Aviation and Transportation Security Act of 2001. While much could be said about ALPA's many ongoing security-related initiatives, the following examines just a few of the numerous projects whose focus is either on, or related to, human factors.

The first and most urgent need immediately after September 11 was that of helping airline crew members who were experiencing significant stress

as a result of the attacks. ALPA's trained peer support volunteers provided Critical Incident Stress Management (CISM) assistance to these pilots during the first few days after September 11, and further assistance to several individuals during the ensuing few months. CISM centers were established at major airports and domiciles to interview and discuss what had transpired with hundreds of crews. Because travel was difficult in the immediate aftermath, volunteers from each region were provided with the necessary information to assist crew members. The CISM Program is an outgrowth of ALPA's very successful Critical Incident Response Program.

A fundamental and obvious security improvement needed immediately after September 11 was an overhaul of the government/industry anti-hijacking procedure, known as the "common strategy." The common strategy was developed initially in the 1970's by the FBI, airlines and ALPA to deal with hijacking threats initiated in flight. It represented a set of procedures based upon a plan of capitulation to virtually all hijacker demands and worked well for thwarting hijackers with long delay tactics and effective negotiations. It was never intended to, nor could it, prevent hijackings committed by suicidal fanatics. Recognizing the inadequacies of the old common strategy, ALPA convened and chaired numerous meetings with government and industry representatives from late 2001 to early 2002 to create a new strategy. The new common strategy was developed to recognize and respond to four different levels of threat that can be posed both on the ground and in flight. It includes protective measures for the flight deck and cabin, better flight deck-cabin communications, and greater reliance on proper crew resource management. Obviously, there were numerous human factors issues associated with its development. Airline crews are now being trained on the new common strategy.

*continued on page 23...*

# Unleashing the Power of Human Performance through Technology: Air Force Applications to Aviation Security Issues

Tamara L. Chelette, Ph.D.  
Daniel L. Kugel

**T**he Human Factors elements of Air Force research and development, which are now mostly gathered under the umbrella of the Air Force Research Laboratory (AFRL), have historically transitioned technology to the general market in advance of, or in tandem with, the transition to the warfighter. Examples of such transition paths include simulated 3-D audio displays, active noise reducing headsets, miniature cathode ray tubes, and human fatigue countermeasures. In this field, these transition methods are frequent because of the pervasive commercial applicability of innovative human factors technology. In contrast, society would likely be poorly served if developers of lethal weapons or space vehicles followed such a course. Yet this transition path has often been misunderstood and maligned precisely because it appears to lack focus on solving military-unique problems.

During the last year it has become apparent to our nation that the military's problems are not so unique. Every agency, every municipality, every citizen, and every visitor is now aware of the need for increased security measures, threat recognition, infrastructure protection, and biodefense medicine. As experienced brokers of human centered technology to commercial American society, human factors specialists in the Air Force Research Laboratory are now engaged in bringing their expertise to the challenges of Homeland Security.

In October 2001, AFRL responded to the President's call for improved, integrated homeland defense by developing a web-access database of current projects that could be transitioned to other agencies to help counter terrorism. Approved government agencies can view and sort the portfolio by source, maturity of the technology, funding status, or envisioned application. Technologies are grouped into four major thrusts, one of which contains aviation safety related enhancements. Approximately ten percent of those programs were identified by the Human Effectiveness Directorate, the human factors experts of the Lab.

For example, the Air Force has been in the practice of operating out of secure bases with little experience in flight operations from public places. But now the technologies that have been deployed to secure those bases could be applicable to airports, aircraft, and control towers. Technologies in the Lab that are ready for this application include the following. Biometrics that uniquely identify personnel using ocular scan devices could be used at employee and ticket check-in. Distributed mission training simulators would allow geographically dispersed security teams to rehearse scenarios together. Improved night vision devices that have natural fields of view, improved contrast sensitivity, reduced weight, and un-tethered multi-sensory information display could provide pilots, security personnel, and air traffic controllers continued capability in airport power outage emergencies. Operations designed to use non-lethal weapons are under development that can disable and disarm a terrorist while in a crowd. A cognitive engineering based integrated control center, designed to provide decision making support to information saturated NORAD monitoring crews, could also be transitioned to city emergency operations centers. A fatigue avoidance scheduling system, designed to manage the schedules of airfield operations, can similarly be used to predict and manage the vigilance of a crew of airport security personnel. The Air Force research program in chemical and biological weapons is focused on detection and safe elimination, thus the AFRL has

*continued on page 24...*

*Tamara L. Chelette, Ph.D., is a senior biomedical engineer and principle investigator for the Air Force Research Laboratory (AFRL) Human Effectiveness Directorate. Dr. Chelette has conducted and published research in the areas of pilot response to sustained acceleration, spatial and visual perception in inertial environments, and biomechanics.*

*Dan Kugel is the Chief of Homeland Defense and Combat Support Sector of the Air Force Research Laboratory (AFRL) Plans and Programs Directorate. He is responsible for the AFRL research portfolio in support of warfighters, peacekeepers, and emergency responders.*



# Special Working Group on Human Factors in Homeland Defense

CDR Andrew H. Bellenkes, Ph.D.  
MSC USN

*CDR Andrew H. Bellenkes, Ph.D., MSC USN, is a military assistant professor in Human Factors and Mishap Investigation at the School of Aviation Safety, Naval Postgraduate School. CDR Bellenkes has more than twenty-five years of experience in Aviation Human Factors System Engineering and currently heads the Special International Joint Working Group on Human Factors in Homeland Defense.*

The United States has always planned for the possibility of an attack on its territory. However, the tragic events of September 11, 2001, and subsequent bio-terrorism are painful reminders that homeland defense programs must be as diverse in nature and scope as are the threats. American homeland defense policies have been designed to ensure this nation's physical security against attack from without and within. This task will not be simple, considering the plethora of complex security risks and must last a long time. It will create many new challenges to military medicine; the operations, lines of research, and technologies designed to carry out the war against terrorism will be volatile and quickly evolving. A critical goal is to ensure preventive and response-related operational readiness through effective risk management—a priority planning designed to provide security by (1) preventing attack and (2) minimizing injury/loss in the event of attack. Effective risk management for homeland defense presents planners with a complex set of tasks. Identifying the myriad human factors associated with such planning will be crucial to this process but it will be challenging because planners must account for human factors associated with territorial defense (i.e., hazard identification, detection, and handling, incident response readiness, special counter-measures, etc.) as well those who would employ chemical/biological/nuclear weapons of mass destruction (i.e., psychosocial, organizational, and political dynamics, available technologies for weapons design, delivery, and employment, etc.).

A Special Working Group On Human Factors In Homeland Defense was created to address these issues (i.e., terrorism/counter-terrorism, weapons of mass destruction, chemical-biological defense, special operations systems and training, aviation security, etc.). Its members include distinguished military and civilian human factors specialists (physicians, psychologists, social scientists, and engineers) from around the world. The group's products include:

1. **Consultancy:** Group members are available for consultation and tasking by government and industry. They and their sponsoring organizations are a recognized repositories of homeland defense human factors expertise.
2. **Immediate Action Response:** Specific, time-critical issues are addressed and the results disseminated to specific "customers," fellow professionals, and/or the general public, as appropriate.
3. **Education:** On-line and in-person workshops/courses on human factors in homeland defense are developed and implemented. An unclassified panel titled, "The Human Factor in Homeland Defense" is sponsored annually. The first of these was a double-session panel conducted in May, 2002, at the annual scientific congress of the Aerospace Medical Association.
4. **Annual Report of the Special Working Group on Human Factors in Homeland Defense:** Provided to approved individuals and organizations beginning in 2003.

The first meeting of the working group was held in Montreal in conjunction with the annual meeting of the Aerospace Medical Association (AsMA). A panel of Political Scientists and Human Factors experts addressed the unique nature of territorial defense-directed asymmetric warfare as well as the

*continued on page 24...*

# DoD Perspective— Human Systems Technology and Aviation Security

CDR Timothy P. Steele  
MSC, USN


**T**he Human Systems Technology (HST) area within the Department of Defense (DoD) provides enabling science and technology that may be focused productively on improving aviation security capabilities, just as it is focused on improving operational capabilities in a multitude of other application areas. HST is organized into three technical subareas:

1. System Interfaces and Cognitive Processing
2. Protection, Sustainment, and Physical Performance
3. Personnel, Training, & Leader Development.

These three subareas facilitate coordination and oversight of the breadth of HST research conducted within and across the Military Departments and Defense Agencies. All share a common underlying objective, which is to better understand human capabilities and limitations and to apply that understanding to facilitate achieving human intent, whatever it may be. The Defense Technology Area Plan, which can be viewed at <https://dstp.dtic.mil>, provides the best description of the depth and breadth of this technology area.

From an over-arching DoD Human Systems perspective, I would like to offer two assertions that, when their implications are fused, point to a way ahead. Assertion one: The human is the center of all operational capabilities. Assertion two: Increasing scientific and technical specialization demands increasing inter-disciplinary collaboration and cooperation. Human Systems Integration (HSI) concepts, methods, and tools currently provide the most promising practical approaches to ensuring the development and acquisition of useful, useable and affordable systems, regardless of application. Facilitating the systematic and disciplined practice of Human Systems Integration is intrinsic to effective systems engineering, therefore, offers a way ahead for aviation security. ■

*CDR Timothy P. Steele, MSC, USN, is a Navy Research Psychologist. He currently serves on the staff of the Deputy Under Secretary of Defense for Science and Technology as the Assistant Director for Human Systems Technology.*



**Observe this!**

Noldus Information Technology bv  
Wageningen, The Netherlands  
Phone: +31-317-497677  
E-mail: [info@noldus.nl](mailto:info@noldus.nl)

Noldus Information Technology GmbH  
Freiburg, Germany  
Phone: +49-761-4701600  
E-mail: [info@noldus.de](mailto:info@noldus.de)

Noldus Information Technology Inc.  
Leesburg, VA, U.S.A.  
Phone: +1-703-771-0440  
Toll-free: 1-800-355-9541  
E-mail: [info@noldus.com](mailto:info@noldus.com)

[www.noldus.com](http://www.noldus.com)

As a researcher, you have to spend your resources as efficiently as possible. Saving time during the collection, analysis and presentation of observational data can mean a big help. And that's exactly what The Observer can do for you. Whether you are observing live or from video, The Observer offers you an easy and accurate tool for the study of activities, postures, movements or human-system interactions.

**Noldus**  
Information Technology

Innovative tools for behavioral research

<http://iac.dtic.mil/hsiac>

# calendar

## may

**San Antonio, TX, USA. May 4–9, 2003**

**74th Annual Scientific Meeting of the Aerospace Medical Association**

Contact: Aerospace Medical Association, 320 South Henry Street, Alexandria, VA 22314–3579  
Tel: (703) 739–2240 • Fax: (703) 739–9652 • URL: <http://www.asma.org/>

**Munich, Germany. May 7–9, 2003**

**XVII International Annual Occupational Ergonomics and Safety Conference**

URL: <http://www.munich2003.com>

**Augusta, GA, USA. May 12–15, 2003**

**Department of Defense Human Factors Engineering Technical Advisory Group**

Contact: Sheryl Cosing, 10822 Crippen Vale Ct., Reston, VA 20194  
Tel: (703) 925–9791 • Fax: (703) 925–9694 • E-mail: sherylcosing@earthlink.net  
URL: <http://dtica.dtic.mil/hftag>

## jun

**Montreal, Canada. June 16–19, 2003**

**SAE Digital Human Modeling for Design and Engineering Conference and Exhibition**

Contact: John Miller, 755 West Big Beaver Road, Suite 1600, Troy, MI 48084  
Tel: (248) 273–2464 • Fax: (248) 274–2494 • E-mail: dhmc@sae.org  
URL: <http://www.sae.org/dhmc>

**Denver, Colorado. June 22–25, 2003**

**Safety 2003 Sponsored by the American Society of Safety Engineers (ASSE)**

Contact: Jeff Naccarato • Tel: (630) 434–7779, ext. 7916 • E-mail: inaccarato@heiexpo.com  
URL: <http://www.asse.org>

**Johnstown, PA, USA. June 22–26, 2003**

**9th International Conference on User Modeling**

Contact: Peter Brusilovsky, School of Information Sciences,  
University of Pittsburgh, 135 North Bellefield Avenue, Pittsburgh, PA 15260  
Tel: (412) 624–9404 • E-mail: peterb@pitt.edu • URL: <http://www2.sis.pitt.edu/~um2003/>

**Crete, Greece. June 22–27, 2003**

**HCI International 2003: 10th International Conference on Human-Computer Interaction jointly with Symposium on Human Interface (Japan) 2003 5th International Conference on Engineering Psychology and Cognitive Ergonomics and 2nd International Conference on Universal Access in Human-Computer Interaction**

Contact: Maria Papadopoulou, ICS-FORTH • E-mail: administrator@hcie2003.gr  
URL: <http://www.hcii2003.gr>

**Tysons Corner, VA, USA. June 23–25, 2003**

**Human Systems Integration Symposium: Enhancing Human Performance in Naval & Joint Environments**

Contact: American Society of Naval Engineers,  
Attn: HSI 2003, 1452 Duke Street, Alexandria, VA 22314  
Tel: (703) 836–6727 • Fax: (703) 836–7491 • E-mail: meeting@navalengineers.org

# of events

**New York, NY, USA. July 8–10, 2003**

**Eastern Ergonomics Conference and Exposition (EECE)**

Contact: Lenore M. Kolb • Tel: (212) 370–5005, ext. 23 • E-mail: [lkolb@ergoexpo.com](mailto:lkolb@ergoexpo.com)

URL: <http://www.ergoexpo.com/index.asp>

jul

**Seoul, South Korea. August 24–29, 2003**

**The XVth Triennial Congress of the International Ergonomics Association**

URL: <http://www.iea2003.org/>

aug

**Montreal, Canada. September 16–19, 2003**

**SAE Digital Human Modeling for Design and Engineering Conference and Exhibition**

Contact: John Miller, SAE International

Tel: (248) 273–2464 • Fax: (248) 274–2494 • E-mail: [dhmac@sae.org](mailto:dhmac@sae.org)

URL: <http://www.sae.org/hdmc>

sep

**St. Louis, MI, USA. September 23–25, 2003**

**5th Annual Technologies for Public Safety in Critical Incident Response Conference & Exposition**

Contact: Center for Technology Commercialization, Public Safety Technology Center

P.O. Box 11344, Alexandria, VA 22312

Tel: (888) 475–1919 • Fax: (703) 933–0123 • E-mail: [jtelander@ctc.org](mailto:jtelander@ctc.org)

URL: <http://www.nlectc.org/conf/nij2003.html> (beginning 5/01/03)

oct

**Denver, CO, USA. October 13–17, 2003**

**Human Factors and Ergonomics Society 47th Annual Meeting**

Contact: Human Factors and Ergonomics Society, P.O. Box 1369, Santa Monica, CA 90406–1369

Tel: (310) 394–1811 • Fax: (310) 394–2410 • E-mail: [info@hfes.org](mailto:info@hfes.org)

URL: <http://www.hfes.org/>

nov

**Memphis, TN, USA. November 2–4, 2002**

**The Second International Conference on Mobile Health**

Contact: International Mobile Health Association

1058 Haight Street, San Francisco, CA 94117–3109

URL: <http://www.intlmobilehealthassn.org>

dec

**Las Vegas, NV, USA. December 8–11, 2003**

**National Ergonomics Conference and Exposition (NECE)**

Contact: Walter Charnizon, President, Continental Exhibitions

370 Lexington Avenue, New York, NY 10017 • Tel: (212) 370–5005 • Fax: (212) 370–5699

URL: <http://www.ergoexpo.com/index.asp>

<http://iac.dtic.mil/hsiac>



# The Human Factors of Civil Aviation and Transportation Security

Eric C. Neiderman, Ph.D., M.G.A.

*Eric C. Neiderman, Ph.D., leads a branch responsible for human factors in the Transportation Security Administration (TSA) at the William J. Hughes Technical Center in New Jersey.*

Prior to the Pan Am 103 tragedy, the unstated goal in aviation security was to eliminate dependence on human operators by fielding ever more complex inspection machinery. Technology was viewed as a panacea for human performance problems. The inherent flaw in this approach was, and is, that it requires technologies with one hundred percent detection accuracy and zero percent false alarms. Since, this “Holy Grail” is more than a few years away, it must be acknowledged that eliminating people from aviation security is not feasible or realistic now and may not be achievable. Further, because people add strength and flexibility to security systems it is probably not desirable to eliminate them. Thus, people will remain involved in aviation security for the foreseeable future; all decisions about whether a bag will be placed on a plane will rest ultimately in the hands and mind of a human. Paradoxically, human performance issues have become even more critical to overall transportation security system success because the high-technology equipment originally designed to replace humans has instead increased their workload.

Given this reality, specific mandates in the United States Aviation Security Improvement Act of June 1991 and the Aviation and Transportation Security Act of November 2001 established the Transportation Security Human Factors Program. In the TSA, human factors includes all security-system events, activities, and phenomena that are influenced significantly by operational human capabilities and constraints. It encompasses selection, training,

performance certification and assessment, job design, task allocation and workload management, motivation and incentive management, system design and procedures, human interactions with computers and other equipment, perception and attitudes, errors, and health/safety. Systematic consideration of transportation security human factors enhances human contributions to present and advanced technology security systems while accommodating operator constraints. Consequential gains in system performance translate into increased safety for all users of the domestic and international transportation system.

The program currently has major initiatives to enhance people, improve equipment, and maximize throughput. These initiatives correspond to the following mission needs: (1) Restrict the opportunity to bring dangerous devices aboard aircraft and transportation vehicles; (2) Reduce the number of passengers needing special security treatment; and (3) Retain human contributions to overall system performance as individual security components are merged into an integrated technology system.

The Transportation Security Human Factors Program is focusing its current efforts on improving passenger and baggage screening performance with X-ray (see Figure 1) and Computed Tomography (CT) equipment (see Figure 2) through better methods of selection, training, and performance evaluation. A major focus is field test and evaluation of new security equipment (e.g., backscatter microdose X-ray imaging, CT explosives detection systems, and trace detection equipment (see Figure 3) to assess key human factors issues.

Security checkpoints use X-ray technology that was originally designed and implemented to counter the threat of hijacking to locate handguns and weapons. However, the threat to civil aviation and transportation has changed to sabotage and mass destruction through sophisticated threats such as

*continued on page 25...*

# Lesson Learned

Edwin Zedlewski, Ph.D.

**T**he National Institute of Justice (NIJ) is the principal research arm of the Department of Justice. It supports research and evaluation through grants and contracts to improve state and local criminal justice systems. So why did a federal research agency come to work at the World Trade Center along side New York City rescue workers? What unique lessons did we learn?

New York City had plenty of trained rescue workers. NIJ supplied some very different skills. Besides its social science policy research, NIJ sponsors an interesting assortment of technology developments ranging from police communications to DNA testing methods. NIJ dispatched a team of engineers to World Trade Center scene on September 13 at the request of the Director of New York State's Emergency Management Office. As rescue workers tunneled into the debris, they discovered their conventional equipment was inadequate for many situations. The Institute served as a bridge between the rescue workers and roughly two hundred federal laboratories, identifying, finding, and shipping needed specialized equipment as rapidly as possible to the rescue site. We asked the labs not to worry about who would pay—NIJ assumed the liability—and to ship as quickly as possible. They did.

The rescue teams urgently needed to search deep into the rubble for voids where survivors might still be alive. NIJ acquired miniature robot crawlers and mounted them with remote cameras. However, the crawlers proved to be useless in the twisting underground crevices, so NIJ cannibalized the crawlers and mounted the cameras on other platforms including long poles that could be extended and poked into the rubble. The most dramatic was the creation of a "K-9 cam," an adjustable, collar-mounted remote camera. NIJ borrowed the concept from a similar setup developed for drug enforcement operations. Dogs were particularly adept at crawling through tight passages. However, their feet were vulnerable to

broken glass and sharp metal so rescue worker equipped them with special K-9 booties.

The NIJ team supported rescue efforts day and night. They did whatever they could through acquisition and invention to bring useful technologies to bear. One of their grim final tasks was to acquire special freezer vans to store the thousands of DNA specimens that accumulated.

Currently, the Institute is sponsoring research to chronicle and analyze the rescue activities from the World Trade Center and the Pentagon. NIJ will compile the lessons learned and translate them into planning for other first responders. We at NIJ learned a valuable lesson too. Terrorists always have the advantage of choosing the target and the specific method of attack. Every scenario—chemical, biological, radiological, blast, and nuclear—poses different challenges for first responders. No amount of training and technology can anticipate how these specifics will impact general response plans. Response teams must recognize their planning limitations and develop capacities to respond extemporaneously. The unexpected is a certainty. ■

*Edwin Zedlewski, Ph.D., is a Senior Scientific Advisor at the National Institute of Justice. His responsibilities are shaping research and evaluation programs that result in better criminal justice policy and practice nationwide. The views expressed in this article are those of the author and do not necessarily reflect the policy or position of the U.S. Department of Justice.*

# Police Performance and Human Factors Research



Bryan Vila, Ph.D.

*Bryan Vila, Ph.D., is Director of Crime Control and Prevention Research, National Institute of Justice, U.S. Department of Justice, Washington, D.C. The views expressed in this article are those of the author and do not necessarily reflect the position or policy of the National Institute of Justice or the U. S. Department of Justice.*

**S**ome of the hottest policing research opportunities in the next decade involve human factors because of its potential for improving officer performance. This is especially important now because local police are the first line of defense for homeland security. There are almost nineteen thousand law enforcement agencies in the U.S. that employ some eight hundred thousand full-time sworn officers at a cost of roughly fifty billion dollars a year, eighty-eight percent of whom work for city, county or state agencies. Most of these agencies are substantially understaffed—in large part because there are too few qualified recruits to replace the large cohort of retiring baby boomers. This problem is being exacerbated by the post-September 11 increase in duties associated with counterterrorism.

All too often, police agencies rely on overtime work to bridge the gap between demand for services and people to provide those services. Even before September 11, some U.S. police officers worked as many as three thousand hours of overtime annually, routinely putting in one hundred-hour work weeks. It is even more common for officers to work double or even triple shifts. If used in moderation, or to respond to short-term crises, overtime can provide a viable solution to police staffing needs. However, overly long or irregular work hours increase fatigue and—as we know from more than a hundred years of research—excess fatigue leads to a host of health, safety and performance problems. Moreover, like the rest of us, tired cops tend to

become more irritable, less discerning, and more prone to make mistakes.

Given the tremendous discretionary powers with which we entrust police, it hardly seems prudent to rely on overtime to bridge the staffing gap. In fact, it's easy to see how too much overtime could trigger a vicious cycle where overly tired officers in police departments are taken out of the available staffing pool because of injuries, illness or just plain burn out; as the staffing pool shrinks, overtime increases and so do fatigue-related losses.

One of the obvious ways out of the dilemma of too few officers to meet demands for critical services is to increase police productivity and improve officers' ability to perform their complex and sometimes dangerous jobs. We also need to do everything possible to reduce early retirements due to on-the-job injuries, illness and burnout. Research supported by the National Institute of Justice (NIJ), the research arm of the U.S. Department of Justice, has made some inroads on officer safety and performance. For example, the now widespread routine use of body armor by police officers is the result of NIJ-sponsored research and development as are many of the tools now available to help officers communicate, process information and handle dangerous suspects and situations.

NIJ's recent research on the prevalence and consequences of police fatigue has opened the door to a host of human factors-related issues. Police departments around the country are beginning to wrestle with work-hour issues such as overtime limits, shift scheduling and compressed shifts. But, guidelines for work-hour practices and fatigue and alertness management have yet to be developed. Other, largely unexplored human factors opportunities include improving the ergonomic fit between officers and their tools and vehicles. Two examples illustrate this point: (1) Patrol cars are essentially tougher versions of family sedans into which a

*continued on page 26...*

# Mitigation is Part of National Security: Potential for Human Factors Contributions to the Improvement of Building Evacuations

Norman E. Groner

**A**s a nation, we are engaged in a vigorous and concerted effort to prevent large-scale acts of terrorism. But what if our Federal government is correct in their assessment that future attacks are inevitable and impossible to prevent? Buildings are logical targets, as they concentrate large numbers of people in relatively vulnerable settings. Although bombs are the most obvious threat, biological and chemical terrorism also require building management and occupants to respond adaptively before professional emergency responders have time to arrive, assess the situation, and begin their responses. Thus, national security depends on well-funded, multi-disciplinary research to develop better responses to extreme building emergencies. The human factors field must be involved, as it has a critically important contribution to make.

To date, there has been limited, but significant progress. Advocacy from citizen's groups, including the World Trade Center Evacuation Study Initiative (WTC/ESI) in which the human factors field is generously represented, yielded long overdue and significant progress in examining building evacuations on September 11, 2001. The National Institute of Standards and Technology (NIST) expanded its investigation of the World Trade Center (WTC) building failures to include evacuations and emergency responders. The federal government recently enacted legislation to create a National Construction Safety Team to investigate significant building failures. It is loosely modeled after the National Transportation Safety Board and will be operated by NIST. The Centers for Disease Control and Prevention is conducting a relatively small-scale epidemiological survey investigating casualties below the impact area in the first of the WTC Towers that was hit. It is also funding the Mailman School of Public Health at Columbia University to conduct a larger and more comprehensive study of social and organizational factors during the evacuations. The National Fire Protection Association is receiving responses to a

mail survey sent to some evacuees and there is a chance that a consortium of three British universities will collect data for the purpose of modeling physical and cognitive ergonomic factors in the WTC building evacuations.

Investigations of extreme building failures are very important, but insufficient. These events are very rare and tend not to replicate. Unlike most other types of technological systems, protective building systems are very loosely coupled and must respond to disruptions of great uncertainty. As an example, uncertainty regarding ignition sources and locations, ventilation, and available fuels make fire behaviors very difficult to predict. Add to this the inherently unpredictable and adaptive nature of terrorist threats, and the futility of protecting against the same scenario is apparent. However, well-conceived research and development is inherently proactive, because designs are conceived to protect against a broad range of scenarios, including those that are imagined, but have never occurred.

Traditionally, the design of building evacuation systems has been dominated by a systems-centered approach where people are conceived as a component that should respond causally to certain inputs. For example, alarms are thought to cause people to start evacuating and failures to take such actions represent inherent human inadequacies and lack of training, if not outright stupidity. However, favorable outcomes from building evacuations necessarily depend on the actions taken by people who are not mechanical systems components that dependably react with assigned

*continued on page 26...*

*Norman E. Groner is an Associate Professor at John Jay College of Criminal Justice, City University of New York. His research interests concern approaches to researching and modeling the cognitive and organization factors pertaining to fire safety and emergency planning.*



## References

- Green, P.M. & Swets, J.A. (1966). Signal detection theory and psychophysics. New York: Wiley.
- Hancock, P.A., Szalma, J.L., Mouloua, M. & Stafford, S.C. (2002). Defeating terrorism using human factors and ergonomics. Paper Presented at 46th Annual Meeting of Human Factors Conference, Baltimore, MD.
- Hancock, P.A. & Desmond, P.A. (2001). (Eds.). Stress, workload and fatigue. Lawrence Erlbaum: London.
- Hancock, P.A. (1998). Should human factors prevent or impede access? *Ergonomics in Design*, 6 (1) 4.
- Mouloua, M., Gilson, R., & Hancock, P.A. (2002). Designing controls for future unmanned aerial vehicles. *Ergonomics in Design*, (in press).
- Parasuraman, R., Masalonis, A.J., & Hancock, P.A. (2000). Fuzzy signal detection theory: Basic postulates and formulas for analyzing human and machine performance. *Human Factors* 42 (4), 636-659.
- Parasuraman, R., Hancock, P.A., & Olofinboba, O. (1997). Alarm effectiveness in driver-centered collision-warning systems. *Ergonomics*, 40, 390-399.
- Szalma, J.L., Hancock, P.A., Mouloua, M. & Parasuraman, R. (2002). Application of fuzzy signal detection to response to terrorism. Paper Presented at 46th Annual Meeting of Human Factors Conference, Baltimore, MD.
- Warm, J.S. (1984). (Ed.). Sustained attention in human performance. Wiley: New York
- Zadeh, L. (1965). Fuzzy sets. *Information and Control*, 8, 338-353.

## ...continued from Hancock article on page 5

two to four seconds) analogous to passengers passing through a reasonably high-speed detection system. Unfortunately, the signal rates typical of laboratory tasks are unrealistically high (e.g., as much as one to two per minute). Thus, laboratory results are likely to under-predict the performance of real screeners as lower signal rates generally result in poorer performance. In the real-world applications the occurrence of signals can be extremely low, perhaps an actual rate of one signal per ten years. Even after the recent catastrophes, government reports show that detection of actual threats remains remarkable low, demonstrating the continuing challenge of the problem. The fact that the actual success (or failure) rates are hidden may be one of the greatest protectors of the security process.

Parasuraman, Hancock, and Olofinboba (1997) addressed the problem of very low signal rates in their work on collision avoidance systems where the probability of a driver having a rear-end collision is estimated at one collision per fifty driving years. Faced with a vast dominance of non-signals, even very sensitive detection systems commit many false positive and even more false alarm responses. In the aviation security situation, false alarms would represent individuals who are singled out from the stream of passengers for further investigation, but who in reality pose no threat. Most passengers shrug off such extended evaluation as the contemporary price of safe travel, but this attitude is not likely to continue. A half century of vigilance research provides a sound database from which specific recommendations for security improvements can be made (Harris, 2002).

Recent techniques for analyzing detection performance, such as fuzzy signal detection theory (FSDT) can enhance the assessment of real-world systems. FSDT combines traditional signal detection theory (Green & Swets, 1966), with the mathematical specifications of fuzzy set theory (Zadeh, 1965), to generate fuzzy signal detection theory (Parasuraman, Masalonis, & Hancock, 2000). It formally per-

mits events to be represented by a continuum, rather than by discrete, signal/nonsignal categories and allows observers to express uncertainty (e.g., "this is probably not a threat but I'm not absolutely sure"). FSDT incorporates this uncertainty into the detection model, offering a better fit for security concerns. (See also Szalma, Hancock, Mouloua & Parasuraman, 2002). At present, there is but one formal screening (at the security checkpoint) and the possibility of random selection for a second screening prior to boarding. It might be possible to monitor the behavior of individuals more frequently using video camera and machine vision systems, applying repeated, but unobtrusive FSDT assessments between passenger check-in and boarding to provide an on-going assessment of level of target "membership." If repeated observations trigger a threshold level, then the individual would undergo a much more intensive screening process. By making assessment an on-going process, rather than a single "all or none" decision, one could provide superior protection against possible seizure of control from the passenger compartment.

Recent advances in computer control have made it both feasible and practicable to control fly-by-wire aircraft from the ground. Largely under development for unmanned aerial vehicles (UAV's) (see Mouloua, Gilson, & Hancock, 2002), the possibility of ground-based control implies that the pilot on board need not necessarily be in control. With greater penetration of this capability, unauthorized individuals could usurp authoritative control of manned as well as un-manned aircraft. This represents an extreme threat, as the suicide of the perpetrators, seen in the September attacks, might not be required to gain a similar outcome. Human factors methods can be used to lock unauthorized individuals out of such control (See Hancock, 1998) and these efforts need to be pursued to an ever greater degree as efforts to implement datalink, the ground-to-air computer communications system are advanced. If the price of freedom is eternal vigilance, we would do well to know much more about vigilance, where it might fail and what can continue to make it successful. For its failure is not a price we can afford to pay. ■

...continued from Hart article on page 6

relative ease with which inspectors have been able to breach airport security (GAO, 2000) are but a few of the vulnerabilities of the U.S. aviation security system that have become visible to the public eye only recently.

The threats for which security forces must remain vigilant are as ill defined and changing as the identities and characteristics of the people who would do harm and ways in which security might be breached. Potential targets include aircraft, the aviation infrastructure, and thousands of historic, strategic, sentimental, or densely populated structures. Although various human and technology barriers are in place or planned, they provide a security “net” rather than the defense in depth focused on safety. There is rarely more than one form of deterrence to counter each combination of threat vector, threat type, and physical location. Parallel, independent redundancies do not exist and one node of the security net does not share or compare information with the next to enable the growth of evidence from multiple sources. A significant distinction between aviation security and safety is that security measures must protect against threats that are deliberate and intentional whose timing and location is not random. And they do not occur as a consequence of inadvertent failures that can be prevented by human or technological solutions once identified.

Despite the difficulty of identifying future security threats, increasingly sensitive and capable information, sensing, and screening technologies are being developed to deter new threats. Human factors can offer technologists and regulators some protection against high-cost, high-tech solutions that do not offer comprehensive and enduring solutions. They can work with the front line—security personnel, ticket agents, pilots, flight attendants and their employers—to identify security gaps and figure out how to ensure that humans are part of the solution in the future, not the problem. Drawing upon knowledge and techniques developed to improve aviation safety, human factors professionals offer established principles for designing better interfaces between humans and machines, computational models and simulations to predict the potential impact of new technologies and procedures, and tools to evaluate the reliability and effectiveness of prototype and fielded systems. Data acquisition and analysis tools could identify deviations from planned routes of flight or contribute to passenger profiling. Data mining and visualization tools could be adapted to convey security information clearly and unambiguously. Human factors has much to offer in selecting the new security workforce and adapting current security personnel, pilot, controller, and

flight attendant training programs to reflect changes in the system. Expertise in organizational and team behavior might be applied to the formation of more effective security teams and mitigate the proliferation of ad hoc responses by pilots and controllers in response to perceived threats. Revised procedures must ensure that the new focus on security does not distract pilots and controllers from tasks necessary to maintain safety; the nation needs a system that is both safe and secure.

The field of human factors has an opportunity to offer its expertise to the solution of a national need. It might infuse the current rush toward technology acquisition with a bit of common sense; single-point security solutions, particularly technologies that cannot adapt to evolving threats, may be relatively easy to defeat. If well selected, motivated, and trained, humans in the security system can provide a flexible and adaptable source of redundancy to the technology that is being rushed into the breach. Years of research have been performed on relevant topics. Thus, the nature of the questions will be familiar—human operators and their interaction with technology—even though the application domain may not be. Human factors professionals, in common with other behavioral scientists, can contribute or stand by and watch, with their integrity intact but their relevance in doubt. ■

## References

- Reason, J. (1997) *Managing the Risks of Organizational Accidents*. Aldershot, England: Ashgate.
- U.S. Government Accounting Office (GAO). (2000). *Aviation security. Long-standing problems impair airport screener's performance (FAO/RCED-00-75)*. Washington, DC: Government Printing Office.

...continued from Endsley article on page 7

used to develop and evaluate system design concepts in very diverse fields applicable to homeland security, including aviation, medicine, and information intelligence operations. It features three main components:

1. SA requirements analysis employs a technology-independent, cognitive task analysis methodology in which the major goals of a particular job are identified along with sub-goals necessary to meet these goals and their associated decisions, and the SA needed to make and carry out these decisions.
2. Application of SA-Oriented Design principles, based on a cognitive model of how people achieve SA in challenging environments, link SA requirements to good system design within a particular domain. Fifty principles have been developed that include direct presentation of higher-level SA, goal-oriented information displays, support for global SA, increased salience of critical cues in prototypical classes of situations used in decision making, and ways of dealing with system complexity, conveying levels of confidence and uncertainty, the design of alarms and advanced automation concepts, and supporting SA in multi-operator and distributed team environments.
3. SA measurement and validation of system designs during iterative test and evaluation is critical to insure system design concepts provide operators with the SA they need. The Situation Awareness Global Assessment Technique (SAGAT) has been used successfully to provide this information by directly and objectively measuring operator SA in evaluating avionics concepts, display designs, and interface technologies (Endsley, 1995). A sensitive and diagnostic tool, this provides a key input designers need for iterating design concepts to overcome any deficiencies.

The SA-Oriented Design process supplements other human factors analysis techniques, design guidelines and measurement approaches to provide a critical linkage to the cognitive foundation of performance in systems operations—the ongoing representation of the current situation that drives decision making and behavior aimed at keeping that environment aligned with operator goals. It provides a foundation for system design based on information content rather than surface features using principles drawn from an understanding of the cognitive mechanisms that both aid and limit our ability to achieve high levels of SA in complex domains. SA-Oriented Design provides a mechanism by which the designer can determine the real information needs of systems operator and can carefully tailor system designs to those needs in a wide variety of homeland defense and security operations. ■

## References

- Bennis, W. (1977). *Thoughts from a victim of info-overload anxiety*. Yellow Springs, OH: Antioch Review.
- Endsley, M. R. (1995). Measurement of situation awareness in dynamic systems. *Human Factors*, 37(1), 65-84.
- Endsley, M. R., Bolte, B., & Jones, D. G. (in press). *Designing for situation awareness: An approach to human-centered design*. London: Taylor & Francis.

...continued from Mumford article on page 8

genuinely interested in behavioral science and we are confident that their advisory council structure will reflect that.

One concern that should unite the grass roots of this field is the proliferation of security technology lobbyists on Capitol Hill. By mid-December 2002, four hundred forty-four registered lobbyists described their interests in terms of terrorism or security. Under that sort of influence, the wellspring of funding will likely to flow to well intentioned, but poorly designed, technological solutions. Those few of us lobbying for human factors are working against tremendous odds and will need all the help we can get from field experts in the months and years ahead. We will need compelling stories of how basic and applied human factors research has contributed to design and operational success and would welcome input from the *Gateway* readership. ■

*...continued from Wright article on page 10*

The FAA required airlines to install better locks on existing cockpit door immediately, install new, advanced-technology doors by April 2003, and consider implementing other aircraft security enhancements, such as cabin video. Human factors considerations associated with these improvements include operating procedures for flight and cabin crew regarding cockpit entry and exit, lighting and visibility of the cabin area adjacent to the cockpit door, positioning of the camera monitor in the cockpit and including the monitor in the crew's cockpit instrument scan.

In spite of these improvements, the majority of ALPA's members believe strongly that another layer of defense is needed to protect the flight deck in the event a door is opened or breached by a would-be hijacker. Both the U.S. House of Representatives and Senate agreed by wide margins with the argument that pilots need to be able to defend the flight deck which, by extension, helps defend the safety and security of thousands of others. ALPA led the way in developing a proposal for arming volunteer, thoroughly screened and well-trained pilots as federal flight deck officers to address pilots' fundamental need to maintain personal well-being and feel prepared to counter an attempted hijacking. Professional airline pilots share many characteristics of law enforcement officers—a high degree of discipline and the ability to remain calm under stress and respond rapidly and accurately to critical situations, to name a few. However, not all pilots are mentally prepared to take a life, even in self-defense. It is our expectation that federal authorities will thoroughly evaluate pilot volunteers to determine their suitability for weapon carriage and use of lethal force. Once selected, federal flight deck officer's training curriculum will include simulated cockpit entries by terrorists to gauge pilots' abilities to respond quickly and properly to eliminate the threat.

To state the obvious, anger is not an emotion crew members should carry onto the flight deck. Unfortunately, there have been numerous reports of pilots angry about their security checkpoint experiences with impaired ability to focus on their jobs. While there may be debate over who is to blame for the circumstances, there should be no debate that steps should be taken to reduce causes of pilot frustration and stress just prior to flight. ALPA has long recommended a universal access system to positively verify the identity and employment status of all aviation industry workers to replace manual with electronic screening. Long lines at screening checkpoints and the loss of airline customers who do not wish to be subjected to aggressive new screening procedures have finally led airlines to endorse a transportation-worker

identification card system now under development by the Transportation Security Administration.

Curiously, despite all the praise lavished on El Al Airlines' security measures, the US is giving scant attention to one of the fundamental security measures employed by that airline. In Israel and elsewhere, behavioral profiling is performed by well-trained individuals. They interview selected passengers so their answers, body language and other cues reveal whether they are telling the truth or might have been duped by someone else. One of the well known successes of this technique in keeping bombs and dangerous weapons off aircraft occurred in April 1986 when Nezar Hindawi attempted to send his pregnant girlfriend on an El Al flight from London with a bomb in her suitcase. Although the device had not been discovered during X-ray screening, profilers suspected something was amiss, searched her possessions, and found it. Based on past experience, and the potential for suicide bombers to board aircraft with undetected improvised explosive devices, federal authorities should give strong consideration to implementing behavioral profiling as a component of screening checkpoint security.

These are but a few of the many examples of ongoing efforts that rely upon proper recognition and application of human factors principles. ALPA intends to remain in the forefront of the public discourse on aviation security and promote its security blueprint that recognizes, and endeavors to maximize the benefits of the human element. ■



...continued from Chelette article on page 11

several biotech sensor systems in development that are capable of remotely sensing toxins and pathogens. Finally, the Human Effectiveness Directorate is a world leader in research concerning adversarial and culturally-sensitive behavior modeling.

The AFRL recognizes that homeland defense involves a broad application of Air Force core competencies including force protection, emergency response, and contingency operations. Multidisciplinary integration is the key to turning these promising human-centered technologies into robust solutions. Thus the Lab has restructured its headquarters staff, designating the Combat Support and Homeland Defense Sector to identify, advocate, and manage investment strategies in these lines of research.

In summary, the Air Force Research Laboratory has a distinct capability in human factors research and design that can, and will, be applied to the immediate requirements of aviation security. ■

...continued from Bellenkes article on page 12

challenge of providing defenses against and responses to the use of weapons of mass destruction (WMD). Some specific areas discussed by working group members included:

**1. Identifying the Threat:**

Panelists discussed homeland defense policy and the use of operational risk management as a priority (rather than reactive) process to identify and implement controls against terrorism, described WMD threats, and demonstrated how a proactive approach could be facilitated by a homeland defense-specific databases. Such repositories might be similar to that being developed for the Department of Transportation and contain counter-terrorism resources for each WMD threat.

**2. Response to WMD Incidents:**

The Chemical Biological Incident Response Force (CBIRF) was introduced. It is a unique mili-

tary unit with a consequence-management mission. It employs a host of human and technological resources to provide rapid and effective responses to WMD incidents, thereby limiting the extent of damage and injury from an attack.

**3. Employment of Special Forces in**

**Homeland Defense:** The use of Special Forces troops to prevent threats from reaching the nation and respond to them once they have been described as was the host of challenging human factors issues that they face to accomplish their mission.

The next meeting of the special working group will be held in conjunction with the annual congress of the AsMA in San Antonio, Texas, in May 2003. The theme of meeting will be "Strategies in the Defense Against Weapons of Mass Destruction." If you are working with or have an interest in some aspect of Homeland Defense, and any of the many issues associated with this massive undertaking, please consider participating in this new working group or attending the panel discussion it will sponsor at AsMS meeting. ■

For more information about the 'Human Factors in Homeland Defense' working group, please contact:

CDR Andrew H. Bellenkes, Ph.D. MSC USN  
Phone: (831) 656-2581  
E-mail: ahbellen@nps.navy.mil

Portions of this article have appeared in the June, 2002 issue of NPS Research.

The contents of this article reflect the opinions of the author and do not necessarily reflect those of the United States Department of Defense, the United States Navy, and/or any other agencies of the U.S. Federal Government.

...continued from Neiderman article on page 16

improvised explosive devices. X-ray technologies at security checkpoints are not optimal for locating and detecting such rare and unique targets embedded within a visually cluttered environment. An extensive body of research evaluating target acquisition and signal detection demonstrated conclusively that low target frequencies result in reduced operator vigilance and decreased detection performance. Thus, the TSA recognized that security screeners require an innovative approach to enhance their target detection capability and performance in addition to continually upgraded equipment.

A major effort of the Transportation Security Human Factors Program has been the development of Threat Image Projection (TIP). TIP provides the capability to insert fictional threat images into X-ray and CT image displays of actual passenger bags to increase screener vigilance and measure system detection performance. The TIP system, available for several X-ray and CTX machines, has a number of applications for human engineering test and evaluation. TIP performance data are being used to validate selection testing and screener training and to set accomplishable, real-world performance standards. As a result, individual operator performance data can be used to tailor recurrent training and assure that performance standards are met. System detection capabilities and limitations can be evaluated and fed back to further enhance equipment designs and interfaces. Lastly, TIP permits real-time assessment of system-wide target detection performance and operational evaluation of new technologies, interventions, and procedures.

New security technologies are being developed by manufacturers throughout the world. Such independent development beneficially expands the manufacturing base, but also results in a patchwork of airport equipment. Given the lack of industry standardization, there is a critical need to effectively integrate diverse new technologies into a unified security system that meets the challenge of expediting passenger flow while providing multiple hurdles of threat detection. To meet this goal for a “checkpoint of the future,” human factors issues must be addressed that include physical layout and operator location, placement of controls and displays, allocation of functions between person and machine, supervisory control, communication, bag tracking, passenger reconciliation, deterrence, and screener workload. These issues are further complicated by constraints unique to each airport or transportation node. The human factors issues associated with security integration must be considered carefully, as they probably represent the

largest single impediment to operational system effectiveness. New security technologies must consider integration with both the operator and the environment seriously or they are doomed to under-utilization and ineffectiveness.

All security technologies in use worldwide share one characteristic: The ultimate decision if a bag or passenger will be permitted on an airplane or accepted into the transportation system, rests in the mind of a human. Thus, continued improvements in transportation security require human factors interventions to further enhance person-machine performance. Airport and transportation-system security involves a complex system of trained personnel, properly maintained and calibrated equipment, deterrence, and appropriate procedures to provide multiple layers of security. The need to allow ready access to the public while preventing persons with malicious intent from penetrating secure areas presents a challenge. Applying human factors research and expertise in the design, development, and evaluation of security technologies and systems will ensure that human performance limits are not exceeded human abilities are leveraged to their full benefit in the system. ■



**Figure 1. A typical late-model airport X-ray machine.**



**Figure 2. Computer-tomography aviation security equipment (the CTX5000).**



**Figure 3. Explosive trace detector.**

<http://iac.dtic.mil/hsiac>

*...continued from Vila article on page 18*

variety of communications, weapons and emergency equipment has been jammed along with barriers to hold arrestees in the back seat. Although these sedans tend to be faster and have better handling qualities than many others, they still are ill suited for the dynamic and sometimes hazardous demands of police work. (2) Handguns also are an ergonomic nightmare, even though they are the most pervasive deadly weapon in policing. They are difficult to shoot accurately beyond a few meters even under the most ideal circumstances, although their bullets travel much farther. In dynamic combat situations that combine running, ducking for cover, poor light, and extreme fear with a moving target, officers' bullets hit their opponents less than 30% of the time.

There are too few police officers and not enough qualified people to replace those who are retiring. This problem is expected to persist for at least the next decade and, unless dealt with thoughtfully, may weaken domestic security efforts substantially. One of the best potential approaches to dealing with police staffing shortages is to use the same kinds of human factors research that have added so much to safety and performance in manufacturing, the transportation industry and national defense to enable officers to accomplish more and do it more safely. ■

*...continued from Groner article on page 19*

predetermined responses. Instead, people select and process information that helps them pursue their goals of adapting to stressful, ambiguous, and dynamic situations. To account adequately for the goal-seeking information-processing reality of human behavior, a user-centered design approach will be needed, whereby peoples the real-world roles and responsibilities need to be supported by improved technology, job design, and cooperation.

The following research questions beg for funding and the inclusion of human factors professionals: (1) How do people and emergency responders really use exit stairs? Should they be wider,

how much wider, where, and in what buildings? (2) Are phased and partial building evacuations still psychologically acceptable, or do we need to design for simultaneous, whole-building evacuations? (3) How can technological innovations help people decide when it is safe to leave apartments and hotel rooms and enter corridors? (4) How can signage and way finding aids be improved to reveal emergency routes of egress? (5) How can innovative technologies and procedures help building occupants decide which egress routes are tenable, when to refuge or remain in their present locations? (6) What are the technological and procedural innovations needed to use elevators during building emergencies? (7) How can trained civilian emergency responders (e.g., fire safety directors, floor wardens) be better prepared and what types of technological and procedural support will enable them to achieve good situation awareness and make good decisions? How can they plan and coordinate their responses better with professional emergency responders, emergency managers, public health officials, building tenants and managers, occupants, and visitors? (8) How can persons with disabilities and the people who assist them be better protected? (9) How can training, inter-organizational cooperation, and innovative technologies and procedures better support professional emergency responders who must assess situations and decide on optimal responses? ■

Product Name	Unit Price
50 Years of Human Engineering Book	N/C
50 Years of Human Engineering CD	\$20.00
Anthropometric Data Analysis Sets (ADA)	\$100.00
Application of Human Performance Models to System Design	\$60.00
Biological Psychology Special Issue	\$25.00
CASHE: PVS Software for MAC Computers	\$395.00
Colloquium Videotapes	\$25.00
Color in Electronic Displays	\$45.00
Electronic Imaging Proceedings	N/C
Engineering Data Compendium including User Guide	\$295.00
Engineering Data Compendium User Guide ONLY	\$85.00
HSIAC Gateway Newsletter	N/C
Human Factors Definitions	N/C
NASA TLX Paper & Pencil Version	\$20.00
NASA TLX Computer Version (DOS Version)	\$20.00
Perception & Control of Self Motion	\$29.95
SOAR: Analysis Techniques for Human—Machine System Design	\$45.00
SOAR: Behind Human Error	\$39.00
SOAR: Cognitive Systems Engineering in Military Aviation Environments:	\$45.00
SOAR: Computational Models of Human Performance	\$39.00
SOAR: Human Factors Engineering in System Design	\$35.00
SOAR: Improving Function Allocation	\$39.00
SOAR: Naturalistic Decision Making	\$35.00
SOAR: The Process of Physical Fitness Standards Development	\$45.00
SOAR: Situational Awareness in the Tactical Air Environment	\$45.00
SOAR: Strategic Workload	\$35.00
SWAT (DOS Version)	\$50.00

If you have any questions concerning this product list, please access our web page at <http://iac.dtic.mil/hsiac> or contact Lisa McIntosh at (937) 255-4842, DSN 785-4842, fax (937) 255-4823 or E-mail [lisa.mcintosh@wpafb.af.mil](mailto:lisa.mcintosh@wpafb.af.mil)

<http://iac.dtic.mil/hsiac>



PROGRAM OFFICE  
AFRL/HEC/HSIAC BLDG 196  
2261 MONAHAN WAY  
WRIGHT-PATTERSON AFB OH 45433-7022

DEPARTMENT OF THE AIR FORCE  
OFFICIAL BUSINESS

<http://iac.dtic.mil/hsiac>

(937) 255-4842 Telephone  
(937) 785-4842 DSN  
(937) 255-4823 Facsimile  
(937) 255-2558 Gov. Tech Manager

Thomas Metzler, *Director*

Dr. Joe McDaniel, *Gov. Technical Manager*

Tanya Ellifritt, *Assoc. Gov. Technical Manager*

Dr. Kenneth R. Boff, *Gov. Technical Director*

Human Systems IAC **GATEWAY** is published and distributed free of charge by the Human Systems Information Analysis Center.

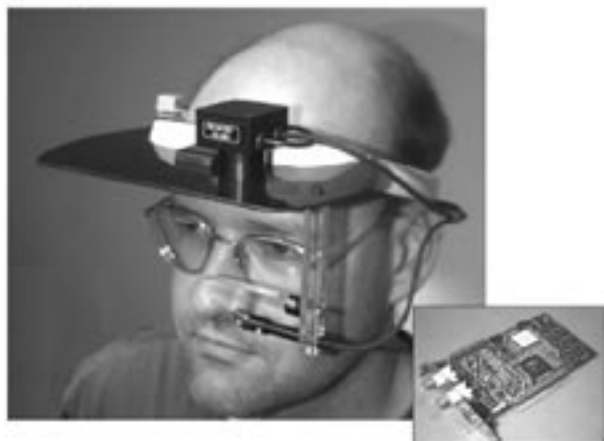
RoseAnn Venis, *Editor*

Ahnie Senft, *Art Director*

Holly Shipley, *Graphic Artist*

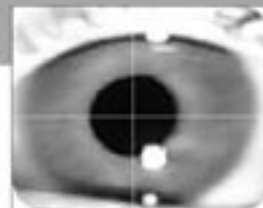
# ISCAN<sup>®</sup> EYE MOVEMENT MONITORING SYSTEMS

ISCAN is the world's leading producer of video based eye movement monitoring systems. Since 1980, our broad range of products has set the pace for performance and usability in wide ranging research, military and medical applications. We can provide off-the-shelf or customized solutions to suit virtually any human factors application.



## Products & Features Include:

- \* Non-invasive, high resolution, real-time measurement of eye position, pupil size and subject's point of gaze.
- \* Complete Eye and Head Tracking Laboratories, with optional Benchtop, High Speed (up to 240Hz) and High Resolution versions available.
- \* Integrated Eye/Head Tracking in VR Displays.
- \* Ultra Lightweight Head Mounted Eye and Scene Imaging Systems.
- \* Specialized Remote Mounted Eye Imaging Systems for Long or Short Range Applications.
- \* Advanced PCI Bus Eye Tracking Electronics.
- \* Complete Data Acquisition Hardware and Analysis Software for Determination of Subject's Visual Performance.



**ISCAN, Inc.**  
89 Cambridge Street  
Burlington, MA 01803 USA

**Tel:** 781-273-4455 **Fax:** 781-273-0076  
**Web:** [www.iscaninc.com](http://www.iscaninc.com) **eMail:** [info@iscaninc.com](mailto:info@iscaninc.com)